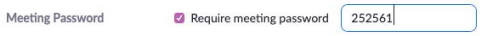
Zoom Security Setting Protocols
Updated 07 Dec 2020

- Use passwords - can be numbers, letters or combination



- Do not select “join before host”

- Choose “host only” for screen share (if another participant needs to screen share, they can be elevated to co-host by the host)

- **Do not embed password** in the meeting link (setting in Zoom to be changed) Example: https://us02web.zoom.us/j/87396276033?pwd=aWpuekV2SUlwQURwcHdJSGU5NGo2Zz09

- Choices for posting events online links - recommend changing current Events and Committees Calendar entries
    - **Preferred method** No clickable link (example)
        Zoom Meeting: https://zoom.us
        Meeting ID: 873 9627 6033
        Password: 12345

    - If clickable link - link cannot include password (example)
        https://us02web.zoom.us/j/87396276033
        Password: 12345

- Recommendation for WSO hosted events (Suggested settings above)
    - Flyer include statement that in case of “Zoom Bombing”, meeting may be locked for a few minutes until intruders have been removed
    - Tech team use Zoom bombing protocols (see Appendix A)

Appendix A: WSO Tech Protocols for Potential Zoom Bombing

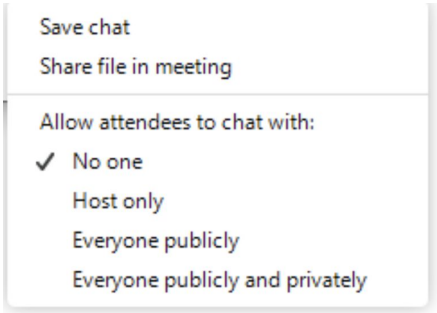
Preferred Technical Setup

1. If the meeting has over 50 attendees, it is helpful to have more than 1 person doing technical support for the meeting. (as host and/or co-host)
2. Let the meeting presenters know, before the meeting begins, that in the case of an incident, you will unmute and start the protocols.
3. When planning the meeting, let the potential attendees know that if the meeting room is locked, there has been an incident and the room will be reopened once the threat has been dealt with.
4. The technical team should be familiar with these protocols and using a computer or laptop (versus phone or tablet) in order to address the situation more effectively and efficiently.
5. If a member of the technical team needs to step away, notify the other team members.
6. If there are multiple technical team members, plan ahead of time who will deal with the video, audio and chat aspects of the incident.
7. If there are multiple technical team members, plan ahead of time who will unmute, narrate and verbally coordinate the protocols.
8. Have the technical team in place, before participants enter the meeting.
9. Ask that technical team and other members assist in taking screenshots of the offending behavior that can be used to report individuals to Zoom.

Zoom Security Setting Protocols
Updated 07 Dec 2020

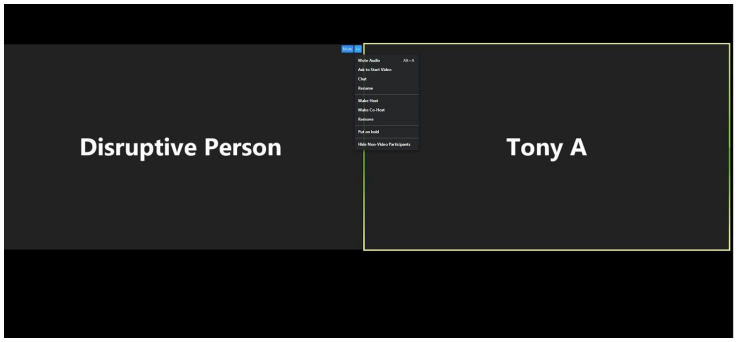
Protocols when a disturbance occurs

1. Tell everyone that you will handle the disturbance. This reduces panic amongst attendees and assists in the coordination of technical tasks to address the situation.
2. Ask participants to take screenshots of offending behavior and send to the tech host who will be reporting.
3. Disable chat - Chat -> “More” dropdown options



4. Click the Participants Button, click the three dots (there may be more button that needs clicked first), and then select the following:
    a. Uncheck allow participants to unmute themselves
    b. Uncheck allow participants to rename themselves (if zoom bomber keeps rotating names it will be more difficult to remove that person)
    c. Check Lock Meeting
        i. Let’s other bombers that may be in the waiting room know that no more bombers are getting in and they should go elsewhere
        ii. If the waiting room has been disabled, this is crucial to keep multiple bombers from overrunning the room

5. Find the offending participants' image
    a. Mute them
    b. (Optionally) Use the three dots to stop their video
6. Click the Security Icon and Choose "Report"
    a. Select the name of the the participant being reported
    b. Check the reason for the report and any comments to provide more information
    c. Upload file to add screenshots or include a desktop screenshot
    d. Click send
7. Remove the offending participant - either by:
    a. Click the Security Icon and choose "Remove participant"
    or
    b. Use the three dots to select remove (may also be done from the participants menu)
        i. Removed participants may not rejoin the meeting--so be sure you have the right person before selecting remove



After removing the disruptor(s)

1. Click the Participants Button and from the three dots menu recheck allow to unmute and change name.
2. Return chat to previous settings
3. Tell everyone what happened and what you did
4. You may want to continue the meeting with the room locked for a while
5. If you need to let in more attendees make sure the waiting room is enabled (participants button, three dots menu) and unlock the room and admit the attendees

Zoom Security Setting Protocols
Updated 07 Dec 2020

How do zoom bombers gain entrance to your meeting?

1. Method 1: Random trying of Zoom meeting ID's / automated number generator -
    a. This can be blocked by having a passcode for all meetings

2. Method 2: Finding a meeting's Zoom info on websites
    a. Do not post Zoom login info in public areas (e.g online calendars) unless absolutely necessary. Preferably email login info to attendees

    b. If it is necessary to post login info, do not post a link with an embedded password as some zoom bombers use scanners that zero in on these types of links. It is suggested to simply post the meeting number and password without a link.